✓ FILED ___ ENTERED
___ LOGGED _____ RECEIVED
8:50 am, Jan 04 2024
AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY R.M. Deputy

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**
**(Northern Division)**

IN THE MATTER OF THE SEARCH OF CERTAIN DEVICES STORED AT THE FBI BALTIMORE, MARYLAND OFFICE, 2600 LORD BALTIMORE DRIVE, WINDSOR MILL, MARYLAND 21244

Case No. 23-mj-3153-ADC

# AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A SEARCH WARRANT

I, Patrick Ramone ("your Affiant"), Task Force Officer with the Federal Bureau of Investigation, being first duly sworn, hereby depose and state as follows:

## INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—nine electronic Devices—that are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. Your Affiant is a University of Delaware Police ("UDPD") Officer and has been one since January 2008. Your Affiant graduated from the New Castle County Police Training Academy on July 31, 2008, and has been a full-time Task Force Officer ("TFO") with the Federal Bureau of Investigation ("FBI") Joint Terrorism Task Force ("JTTF") since July 1, 2019. Your Affiant is currently assigned to the FBI's Baltimore Field Office, Wilmington Resident Agency, National Security Squad, and has received extensive training and experience in the investigation of international terrorism and domestic terrorism violations. Your Affiant is an "investigative or law enforcement officer" of the United States within the meaning of 18 U.S.C. § 2510(7) who is

empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Titles 18 and 21 of the United States Code.

3. The information contained in the affidavit is based, in part, on your Affiant's personal knowledge and observations during the course of this investigation, information provided to your Affiant by other law enforcement officers, and a review of various documents and records. This affidavit is based upon your Affiant's training and experience as well as that of other law enforcement officers working with your Affiant in this investigation.

4. There is probable cause to believe that Kyle STEVENS ("STEVENS") has committed violations of 18 U.S.C. § 2252A(a)(2) (receipt of child pornography), and 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography) (the "TARGET OFFENSES"). There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Please note that this search warrant request arises out of an earlier investigation, as detailed in ¶s 8-13 below, of STEVENS for offenses relating to cyber stalking, sending threats through foreign commerce, and Covid-19 relief program fraud. In the course of that investigation, while carrying out the review of certain electronic devices that were authorized by a prior search warrant obtained in the District of Delaware (copy attached), the investigators discovered in plain sight child sexual abuse material (CSAM), as set forth in ¶s 9-21 below. At that point, the investigators ceased reviewing these materials, and are now seeking authorization to search those devices as part of the investigation of the child pornography crimes that are the TARGET OFFENSES in this additional and distinct investigation.

## IDENTIFICATION OF THE DEVICES TO BE EXAMINED

6. The property to be searched includes the following nine devices (collectively, the "Devices"):

| Device Number for Reference | Type of Device | Physical Description | Numerical Identifiers |
|---|---|---|---|
| 1 | Laptop | Dell Google Laptop, dark in color | Serial Number 7L0W242 |
| 2 | Laptop | Acer Laptop, black | Serial Number: NXEFUEG00302108EA92N00 |
| 3 | Laptop | Teclast Laptop, silver | Serial Number: 8353S212663404 |
| 4 | PC Tower | Erazer Engineer P10 Medion MT39, black | Serial Number: 10023676010462 |
| 5 | Desktop Computer | HP Desktop, dark in color | Serial Number: 4CE1151FG7 |
| 6 | Cellular Telephone | Samsung Galaxy S6, dark in color, with T-Mobile Sim Card | IMEI: 990007034765[**3** or **8**]77[1] T-Mobile Sim Card Number: 8-94902-40001 86941063-4 B/VE |
| 7 | Cellular Telephone | Samsung Cellular Telephone, dark in color with a multicolored, reflective back | IMEI: 353335110090852 |
| 8 | Cellular Telephone | Samsung Cellular Telephone, dark in color with a red and black case, with a Sim Card of unknown brand | IMEI: 358589940102411 Sim Card Number: 89148000006167101219 |
| 9 | Hard Drive | WD Elements external hard drive | Serial Number: WXC2AA081Z84 |

[1] A crack on the rear of the phone makes it difficult to read whether this digit is a 3 or an 8.

7. The Devices are currently located at the FBI's Baltimore, Maryland Office, 2600 Lord Baltimore Drive, Windsor Mill, Maryland 21244. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

## CASE BACKGROUND

8. During the 2018-2019 school year, STEVENS was a student at the University of Delaware. He met two female students, Victims 1 and 2, and, over the course of months, sent them text messages saying things like "I hate you [Victim 1]" and "Yo [Victim 2], I hope you go to hell you trashy, spoiled scumbag." The University of Delaware Police Department and Newark Police Department opened an investigation into STEVENS and, on December 11, 2019, STEVENS was arrested and charged with stalking and harassment in violation of state law. He pled guilty to harassment concerning Victim 1 and was placed on probation.

9. While on probation, STEVENS applied and was accepted to the University of Freiburg, located in Freiburg, Germany. STEVENS's probation was terminated early so he could attend the University of Freiburg. On or about October 29, 2020, STEVENS left the United States to attend college in Germany.

10. Approximately two weeks after STEVENS moved to Germany, in November 2020, he resumed contacting Victim 1 via email, and continued contacting her through March 2022 via multiple email accounts and social media platforms. In September and October 2021, STEVENS resumed contacting Victim 2, via Venmo, a cell phone application. The messages, further described below, repeatedly referenced STEVENS hating and wanting to harm Victims 1 and 2.

11. As a result of STEVENS's messages to Victims 1 and 2 while he was abroad in Germany, the FBI opened an investigation into STEVENS for cyberstalking and sending

threatening communications in foreign commerce. During that investigation, the FBI obtained warrants to search STEVENS' email accounts (Case Nos. 21-311M, 21-312M, 21-313M, signed by United States Magistrate Judge Sherry R. Fallon on November 12, 2021) and Facebook accounts (Case No. 22-265M, signed by then-Chief United States Magistrate Judge Mary Pat Thynge on August 22, 2022).

12. The FBI also discovered that, in 2021, STEVENS submitted ten fraudulent applications to the U.S. Small Business Administration (the "SBA") and/or its authorized lenders in order to obtain loans through small business loan programs established by the passing of The Coronavirus Aid, Relief, and Economic Security Act, also known as the CARES Act. Five of those loans were funded for a total of $1,428,664.14, through the SBA programs targeted at relief for small businesses. The applications were made on behalf of five entities which Stevens purported to own and control. Each of the loan applications falsely claimed that Stevens' businesses had a number of employees, gross revenues, and were in operation at the start of the Coronavirus Pandemic. In fact, the businesses did not exist.

13. On July 14, 2022, a federal grand jury sitting in the District of Delaware returned two Indictments respectively charging STEVENS with (1) two counts of stalking, in violation of 18 U.S.C. § 2261A(2), and five counts of threats in foreign commerce, in violation of 18 U.S.C. § 875(c) (Indictment 22-65), as well as (2) ten counts of wire fraud, in violation of 18 U.S.C. § 1343, and seven counts of money laundering, in violation of 18 U.S.C. § 1957 (Indictment 22-66). An arrest warrant was issued for STEVENS on July 15, 2022.

14. On October 12, 2022, the government issued a request to Germany to extradite STEVENS to the United States to stand trial on the two Indictments for stalking and threats and separately for wire fraud. The United States also requested, pursuant to the United States-Germany

Mutual Leal Assistance Treaty (MLAT), that at the time of STEVENS's arrest for extradition, German law enforcement seize electronic devices found on STEVENS's person, in any bags near his person, in his home, or in his vehicle in a manner consistent with German law.

15. On March 15, 2023, German authorities arrested STEVENS and seized nine electronic devices from him or areas under his control pursuant to the MLAT ("the Devices"). After that time, these electronic devices have been secured in German law enforcement custody and STEVENS has completed extradition proceedings in the German court system.

16. On May 10, 2023, the government received notice that Germany completed its extradition proceedings and had formally granted the request for STEVENS's extradition. On May 23, 2023, your Affiant and other law enforcement personnel travelled to Germany to take STEVENS into custody and retrieve the Devices. Your Affiant returned to Delaware with STEVENS and the Devices on May 25, 2023.

17. The Devices brought back from Germany were initially stored in an evidence locker at the FBI's Wilmington, Delaware Office. On June 5, 2023, United States Magistrate Judge Sherry R. Fallon signed a warrant to search the Devices for evidence of stalking, in violation of 18 U.S.C. § 2261A(2), threats in foreign commerce, in violation of 18 U.S.C. § 875(c), wire fraud, in violation of 18 U.S.C. § 1343, and money laundering, in violation of 18 U.S.C. § 1957 (Case No. 22-252M) (the "First Warrant"). This first warrant and the supporting Affidavit are attached hereto as an exhibit and may be referred to by this Court if it desires to have additional information about the information and evidence relating to the investigation and prosecution of STEVENS on the various other matters for which he was under investigation. Please note, however, that the details contained in ¶s 22-54 and pages 8-23 of that warrant relating to STEVENS's suspected fraudulent

applications for relief funds available under the CARES Act are not pertinent to the current investigation relating to child sexual abuse material ("CSAM") images.

18. Once the warrant was obtained in the District of Delaware to conduct searches on the Devices for information relevant to the matters that were then the subject of federal charges in that District (see ¶ 12 above), the Devices were transferred to the FBI's Baltimore Office and were stored there because that office has greater storage space and a significantly larger Computer Analysis Response Team ("CART") of forensic examiners than does the smaller Wilmington, Delaware Resident Agency ("RA"). In my training and experience, I know that the Devices have been stored at the FBI's Baltimore office in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the FBI. The FBI Baltimore CART team has been responsible for extracting data from the devices and sending that data to case agents in Delaware who have conducted their review.

19. Although the FBI's Baltimore field office has a significantly larger CART than does the Wilmington office, it also fields a substantially greater volume of examination requests. Its resources and personnel remain limited, and the extraction of data from STEVENS's devices has taken time. Your Affiant has been advised that CART Baltimore's typical backlog to review devices is two to six months from the time the Devices are received, based on number of devices requiring extraction and resources available. Extractions can take anywhere between two hours and five and a half months depending on the Device's encryption status and the size of files that are covered by the scope of the search warrant and to be redacted. In this case, a total of nine electronic devices had been recovered from Stevens or were within his control at the time of his arrest including a hard drive, multiple telephones, and multiple computers. Agents obtained the

warrant to conduct the initial search on June 5, 2023, and CART in Baltimore began producing extracted data from the Devices in compliance with the terms of the previous Delaware warrant on a rolling basis for review by the investigating agents in the stalking and wire fraud cases in late July 2023. In the course of investigating agents' review of that data, in late September 2023, they discovered the video file discussed below, which they believed might be child sexual exploitation material ("CSAM"). As discussed below, investigative agents then stopped reviewing data from the Devices, consulted with subject matter experts to confirm that the material was in fact CSAM and that they should pursue the instant warrant, and began working on the instant warrant. Thus, the FBI has been diligently working on searching the devices as extracted data becomes available.

**PROBABLE CAUSE**

20. Consistent with the First Warrant's authorization to search for "any information related to victims of cyberstalking or threats," the FBI reviewed Device 8's video folder for material related to victims of cyberstalking or threats. The video folder for Device 8 contained 259 videos, a majority of which appeared to be stock videos which came preloaded on the device when it was purchased. However, the video folder also contained a video with the file name "Orange Juice Recipe." The thumbnail image for that video, which showed a preview of its contents, showed what appeared to be a naked human body. Knowing the majority of STEVENS' cyberstalking and threats victims are women, and knowing from training and experience that cyberstalkers sometimes use real or digitally altered images of women to harass them, the FBI special agent conducting the review clicked on the video as within the scope of the First Warrant.

21. The video is approximately two minutes and forty-four seconds in length and depicts one naked prepubescent female and one naked female of an undetermined age laying on a couch. They kiss, mouth to mouth, in various positions. The video then fades out and back in and

shows the same naked prepubescent female and naked female of an undetermined age laying on what appears to be a bed. The female of an undetermined age digitally penetrates the prepubescent female. The video fades out and back in and shows the same naked prepubescent female and naked woman of an undetermined age on the same bed. The prepubescent female is naked and sitting on the lap of the naked female of an undetermined age. The two are kissing. Your Affiant has consulted with an FBI Special Agent who specializes in crimes against children who confirmed that, in her training and experience, the video is child sexual abuse material (CSAM).

22. Your Affiant has probable cause to believe that evidence of STEVENS' receipt and possession of CSAM will be found on the Devices. As set forth above, the FBI has identified a video depicting CSAM video on Device 8. As further set forth below, your Affiant knows, from training, experience, and in consultation with CSAM investigators, that people who obtain CSAM usually download it from the internet and store it, rather than delete it. Because each of the nine Devices has the capacity to both access the internet and store data, and because your Affiant has discovered CSAM on one of STEVENS' devices, your Affiant has probable cause to search all nine devices for CSAM. A further description of the ability of electronic devices to store data for long periods of time appears below under the heading "Electronic Storage and Forensic Analysis."

## DEFINITIONS

23. The following definitions apply to this Affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Chat room," or "chat groups," as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have

the ability to transmit electronic files to other individuals within the chat room.

c. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

d. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

e. "Cloud storage" is an online central storage location that allows users to access their files from anywhere using a device connected to the Internet.

f. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, tablets, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

g. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

h. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware

may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

i. "Hashtag," as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

j. "Computer software," as used herein, is digital information that can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

k. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

l. "Internet Protocol address" or "IP address," as used herein, refers to a numeric or alpha-numeric label used by a computers or other digital devices to access the Internet. For example, Internet Protocol version 4 defines an IP address as a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Another example, Internet Protocol version 6, uses both numbers and letter (e.g., 2001:db8:0:1234:0:567:8:1). Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs", defined below) control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

m. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

n. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

o. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

p. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

q. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

r. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals or pubic area of any person.

s. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

t. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

**Discussion of Child Pornography, Persons who Possess and Collect Child Pornography and How Use of Computers and the Internet Relates to the Possession, Receipt, Transportation, and Distribution of Child Pornography**

24. Based on your Affiant's training and experience and consultation with FBI Special Agents with training and experience related to child pornography investigations, your Affiant has learned that individuals who utilize the internet to view and receive images of child pornography

are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals, including the following:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children frequently maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, or in online storage, email accounts or other online communication accounts, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. This data is typically in digital format, and often maintained on computers and in online storage, email accounts or other online communication accounts.

f. Individuals who would have knowledge on how to distribute and receive digital images of child pornography through the use of Peer-to-Peer networks and other online methods would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.

25. Based on the training and experience of other law enforcement officers with whom your Affiant has had discussions, your Affiant has learned the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers and the internet have added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers and the internet serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Mobile devices such as laptop computers, smartphones, iPods, iPads and digital media storage devices are known to be used and stored in vehicles, on persons or other areas outside of the residence. Small mobile devices such as cellular telephones, web cameras, cameras, film, videotapes, video recording devices, video recording players or other photographic or video equipment, tablets, flash drives, hard drives, or other computer storage devices (hereinafter referred to as "Electronic Devices") may be small enough to be stored and transported on someone's person.

d. Smartphones have the capability to access the Internet and store information, such as videos and images. As a result, an individual using a smartphone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smartphone can also easily plug the device into a computer, via a USB cable, and transfer data files from one digital device to another. Many people generally carry their smartphone on their person.

e. Child pornographers can now transfer photographs from a camera onto a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography.

f. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), easy access to the Internet, and online file sharing and storage, the computer is a preferred method of distribution and receipt of child pornographic materials.

g. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography use online resources to retrieve and store child pornography, including services offered by Internet Portals such as AOL Inc., Yahoo! and Google, Inc., Facebook, Dropbox, Instagram, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, file exchange services, messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Email accounts, online storage accounts, and other online communication accounts allow users to save significant amounts of data, including email, images, videos, and other files. The data is maintained on the servers of the providers and is occasionally retained by the providers after the user deletes the data from their account.

h. In your Affiant's recent investigative experience, as well as recent discussions with law enforcement officers, your Affiant knows that individuals who collect child pornography are using email accounts, online storage accounts, and other

online communications accounts to obtain, store, maintain, and trade child pornography with growing frequency, in addition to, or as an alternative to, the use of personal devices.

i. Based on traits shared by collectors, online storage accounts, and other online communication accounts, the increased storage capacity of computers and server space over time, and the facts set forth below, there exists a fair probability that evidence regarding the receipt and possession of child pornography will be found on the Devices.

j. In addition, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools.

k. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten.

l. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages.

m. The storage capacity of personal computers has increased dramatically over the last few years. Common and commercially available hard drives are now capable of storing over 500 GB of data. With that amount of storage space, an individual could store thousands of video files and/or hundreds of thousands of image files.

n. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Since the storage capacity of hard drives has increased dramatically over the last several years, it is more likely that the above-described information will be recovered during forensic analysis.

## TECHNICAL TERMS

26. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless Devices used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the Devices.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

d. Internet: The Internet is a global network of computers and other electronic Devices that communicate with each other. Due to the structure of the Internet, connections between Devices on the Internet often cross state and international borders, even when the Devices communicating with each other are in the same state.

27. Based on my training, experience, and research, I know that the Devices have capabilities that allow them to serve as a wireless telephone and digital camera and to access the internet, and/or to store such electronic data. In my training and experience, examining data stored on Devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the Devices.

## ELECTRONIC STORAGE AND FORENSIC ANALYSIS

28. Based on my knowledge, training, and experience, I know that electronic Devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the Devices. This information can sometimes be recovered with forensics tools.

29. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files.

Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

30. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage Devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a Device can also indicate who has used or controlled the Device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic Device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic Devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore,

contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a Device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic Device to receive or store CSAM, the individual's electronic Devices will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic Devices are an instrumentality of the crime because they were used as a means of committing the criminal offense. The electronic Devices are also likely to be a storage medium for evidence of crime. From my training and experience, I believe that electronic Devices used to commit a crime of this type may contain: data that is evidence of how the electronic Devices were used; data that was sent or received; and other records that indicate the nature of the offense.

31. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

32. *Manner of execution.* Because this warrant seeks only permission to examine Devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

**CONCLUSION**

33. Based on the foregoing, there is probable cause for this Court to issue the requested warrant.

Respectfully submitted,

*/s/ Patrick J. Ramone Jr.*
Patrick J. Ramone Jr.
Task Force Officer
Federal Bureau of Investigation

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 20th day of December, 2023.

A. David Copperthite
The Hon.
United States Magistrate Judge